IN THE CLAIMS

Claims 1-55 (cancelled)

56. (New) A method for transmission of information with protection against copying with use of a personal cryptoprotective complex, the method comprising:

in a ROM of each of personal cryptoprotective complexes, storing copies of a mother code being a set of random numbers (M1, M2, ..., MN), encryption, decryption and information processing programs, wherein record is carried out in a protected way only in said personal cryptoprotective complexes, said way excluding the possibility of recording to other media and modifying said programs, as well as personal data of a user including his or her electronic signature and other attributes used for execution of cryptoprotective operations and generation of electronic documents, and setting date and time in a built-in clock;

in the input of user's information to the personal cryptoprotective complex, inputting user's commands to establish a mode of processing the user's information, to generate a non-copied electronic document, and processing the inputted user's information;

in accordance with the established mode of processing the user's information and the earlier received information, generating service information by means of the information processing program, and combining the service information with the processed user's information to obtain an electronic document, attributes of the electronic document in the form of service information being separated from the processed user's information by means of service symbols, and in accordance with a user's command to generate a non-copied electronic document, including a command in the service information, said command being intended for the personal cryptoprotective complexes and being in the form of a typical set of symbols inputted earlier to the ROM in structure of the information processing program, and

storing the obtained electronic document in a section of the ROM intended for non-copied electronic documents of the personal cryptoprotective complex;

establishing a protected communication session with application of the personal cryptoprotective complexes on the basis of a single-use key of the communication session generated using random numbers, and inputting a user's command to transmit the non-copied electronic document recorded in the PROM to other subscriber of the established communication session;

encrypting the electronic document by a dynamically transformable daughter code while reading an electronic document inability-for-copying command out of the service information, establishing the protection against modification to the encrypted information, and transmitting the encrypted information to another personal cryptoprotective complex;

upon termination of transmission of the non-copied electronic document, disabling it for a predetermined time period T1 in the PROM according to said inability-for-copying command;

receiving the electronic document and decrypting the electronic document, establishing the reliability of information by check for absence of distortions in said information,

searching for and selecting service information from decrypted information by means of service symbols, using the service symbols to find the service information containing the electronic document inability-for-copying command, recording the electronic document to the section of the PROM intended for non-copied electronic documents, and disabling said document for the predetermined time period T1;

generating an electronic-document-loading-acknowledgement password in the personal cryptoprotective complex of a receiving party and transmitting the electronic-document-loading-acknowledgement password in the encrypted form to the personal cryptoprotective complex of a sending party;

in case if the sender does not receive the electronic-document-loading-acknowledgement password from the recipient during the time period T1, enabling the electronic document in

the PROM of the personal cryptoprotective complex of the sender, while ignoring the subsequent reception of said password;

in case if the recipient does not send the electronic-document-loading-acknowledgement password to the sender during the time period T1, deleting the electronic document from the PROM of the personal cryptoprotective complex;

receiving the electronic-document-loading-acknowledgement password in the personal cryptoprotective complex of the sending party, generating an electronic-document-transmission-acknowledgement password, and requesting a user acknowledgement in response to the sending of the present password to the personal cryptoprotective complex of the receiving party;

in case if the user gives no acknowledge in response to the sending of the password during a predetermined time period T2, then, on the expiration of said time period, automatically enabling said electronic document in the PROM of the personal cryptoprotective complex of the sender, and automatically deleting said electronic document in the PROM of the personal cryptoprotective complex of the recipient;

in case if the user acknowledges the sending of the password during the time period T2, sending the present password in the encrypted form to the personal cryptoprotective complex of the recipient, wherein said electronic document is automatically deleted from PROM of the personal cryptoprotective complex of the sender, and said electronic document is automatically enabled in the PROM of the personal cryptoprotective complex of the recipient when he or she has received said electronic-document-transmission-acknowledgement password, followed by inputting user's commands, establishing a mode of processing the decrypted information according to the user's commands received from the service information and according to the earlier inputted information and the information processing program, and outputting the processed information to the user together with service symbols that authenticate attributes of the received electronic document.

57. (New) The method according to claim 56, further comprising:

receiving decrypted information to the personal cryptoprotective complex, said information being the non-copied electronic document containing a variable face value denoted in a predetermined way by service symbols;

decrypting said information and recording the received electronic document to the ROM of the personal cryptoprotective complex;

determining service symbols in the electronic document by means of the information-processing program;

determining a variable face value information of the electronic document in service information, and outputting said variable face value information to the user;

subdividing the electronic document into arbitrary parts by changing face values of parts using the information processing program in such a manner that their total sum remains invariable, wherein other characteristics and attributes of parts of the electronic document also remain unchangeable;

sending parts of the electronic document to other personal cryptoprotective complexes;

receiving several identical electronic documents with variable face values to the personal cryptoprotective complex and automatically collecting said documents using the information-processing program into a unified electronic document by summing their face values.

58. (New) The method according to claim 57, wherein the electronic document with a variable face value is an electronic bank bill of exchange with a predetermined time for repayment, wherein the service information of said bill contains data of a bank drawn the bill, including electronic digital signatures of the bank generated using a personal cryptoprotective complex, data of a user who has received the bill, currency and a face value of the bill as well as a bill repayment date after which the bank will enable a mortgage amount of money left at a user's

account that will be transferred ahead of time to any holder of the present electronic bill or its part after reception of the electronic bill to the personal cryptoprotective complex of the bank, identify data of the electronic bill and determine its face value, and if the date of repayment indicated in the bill is not later than a current date, the holder will obtain the sum corresponding to the face value of the presented electronic bill.

59. (New) The method according to claim 56, further comprising:

adding a temporary individual number generated by a random-number generator to the electronic document, and an arbitrary inputted value of the time period T2, said number and value being encrypted together with the electronic document;

inputting a command to transmit the electronic document to other user during the protected communication session or in the encrypted electronic letter;

when the transmission of the present electronic document terminates, disabling said document for a predetermined time period T1 in the PROM of the sender and marking said document with an assigned temporary individual number;

in case of failures in transmission of the electronic document, the sender repeatedly sends the present electronic document with the same accompanying data;

receiving the electronic document and decrypting the electronic document, establishing the reliability of information by check for absence of distortions in the information;

searching for and selecting service information from the decrypted information by means of service symbols, using service symbols to find service information containing an electronic document inability-for-copying command and the temporary individual number of the present document; collating said number for presence of a disabled electronic document having the same number in the PROM, and in case if coincidence is absent, recording the electronic document to the section of the PROM intended for non-copied electronic documents, marking it with the

assigned temporary individual number and disabling the electronic document for the predetermined time period T1;

in the personal cryptoprotective complex of the receiving party, generating an electronic-document-loading-acknowledgement password on the basis of a random number, automatically adding said temporary individual number of the present electronic document to said password, recording a password to the PROM, and transmitting the electronic-document-loading-acknowledgement password in the encrypted form to the personal cryptoprotective complex of the sending party during the protected communication session or in the encrypted electronic letter;

receiving the electronic-document-loading-acknowledgement password in the personal cryptoprotective complex of the sending party, finding the disabled electronic document in the PROM, said document being marked by number corresponding to a number received with the password, and in case of presence of the disabled electronic document and coincidence of numbers there is the step of generating an electronic-document-transmission-acknowledgement password with use of electronic-document-loading-acknowledgement password, said temporary individual number of the electronic document being automatically included therein;

requesting a user acknowledgement for sending said password to the personal cryptoprotective complex of the receiving party;

in case if the user does not give acknowledgement for sending the password during an arbitrary time period T2 which value was inputted beforehand by the sender in establishment of an electronic document sending mode, then after the expiration of a predetermined period of time there are the steps of: automatically enabling said electronic document in the PROM of the personal cryptoprotective complex of the sender; and automatically deleting said electronic document in the PROM of the personal cryptoprotective complex of the recipient;

in case if the user gives acknowledgement for sending the password during the time period T2, then sending said password in the encrypted form to the personal cryptoprotective complex of the recipient, wherein said electronic document is automatically

deleted from the PROM of the personal cryptoprotective complex of the sender, and when the recipient has received the electronic-document-transmission-acknowledgement password, there is the step of finding the disabled electronic document and the recorded copy of the electronic-document-loading-acknowledgement password in the PROM of the personal cryptoprotective complex of the recipient, said document and said copy being denoted by number corresponding the number received with the password, and only in case of presence of the disabled electronic document, coincidence of numbers and presence of a direct association between passwords, said electronic document is automatically enabled;

recording the electronic document to the section of the PROM of the personal cryptoprotective complex, intended for non-copied electronic documents and closed for users of the PROM, and deleting said temporary individual number;

in case of failures in transmission of the electronic document or acknowledgement passwords, users carry out the backup of transmission.

60. (New) The method according to claim 59, further comprising:

adding an individual number N1 of the personal cryptoprotective complex where from the electronic-document-transmission-acknowledgement password will be sent, a temporary individual number N2 generated by the random-number generator, and an infinite value T2 of the time period to be inputted by the user, said number and value being encrypted together with the electronic document, to the transmittable electronic document;

inputting a command to transmit the electronic document to other user in process of the protected communication session;

when the transmission of the present electronic document terminates, enabling said document for a predetermined time period T1 in the PROM of the sender and marking said document with said assigned number N2;

receiving the electronic document and decrypting the electronic document, establishing the reliability of information

by check for absence of distortion in information;

searching for and selecting service information from the decrypted information by means of service symbols, using said service symbols to find service information containing an electronic document inability-for-copying command and numbers of said document, recording the electronic document to the section of the PROM intended for non-copied electronic documents, marking said document with its assigned number N2 and disabling the electronic document for the predetermined time period T1;

in the personal cryptoprotective complex of the receiving party, generating the electronic-document-loading-acknowledgement, automatically adding said number N2 of the present electronic document to said password and transmitting the result in the encrypted form to the personal cryptoprotective complex of the sending party during the same or other protected communication session;

receiving the electronic-document-loading-acknowledgement of the electronic document in the personal cryptoprotective complex of the sending party, finding the disabled electronic document in the PROM, said document being marked by number N2 corresponding to the number received with the password, and in case of presence of the disabled electronic document and coincidence of numbers, deleting the present electronic document from the PROM, because the time period T2 is equal to an infinite value;

in the personal cryptoprotective complex whose individual number corresponds to the number N1 assigned to the electronic document, inputting a numerical value corresponding to the number N2 of the electronic document, generating the electronic-document-transmission-acknowledgement password while automatically including therein own individual number corresponding to N1 and the inputted number N2;

sending the present password in the encrypted to the personal cryptoprotective complex of the recipient of the electronic document;

when the personal cryptoprotective complex of the recipient has received the electronic-document-transmission-acknowledgement

password in its PROM, finding the disabled electronic document marked by the number N2 corresponding to the number received with the password, collating the numbers N1 in the electronic document and in the password, and only if coincidence of numbers takes place, automatically enabling said electronic document;

recording the electronic document to the section of the PROM of the personal cryptoprotective complex, intended for non-copied electronic documents, and deleting the added numbers N1 and N2.

61. (New) The method according to claim 59, further comprising:

adding the temporary individual number generated by the random-number generator and an infinite value T2 of the time period, said number and value being encrypted together with the electronic document, to the transmittable electronic document;

inputting a command to generate said electronic-document-transmission-acknowledgement password;

generating an electronic-document-acknowledgement password, assigning a number and a variable face value, if any, thereto, said number and variable face value corresponding to the temporary number and temporary face value of the electronic document;

transmitting the electronic-document-acknowledgement password in the encrypted form during a cryptoprotective communication session to a certain user or keeping said password in own personal cryptoprotective complex;

disabling the electronic document for an arbitrary time period T1 in the PROM of the personal cryptoprotective complex, making copies of the electronic document and transmitting them to other users in process of the cryptoprotective communication session or in an encrypted electronic letter;

after the expiration of the time period T1, deleting the electronic document from the PROM of the sender;

receiving copies of the electronic document, decrypting the electronic document, searching for and selecting service information from the decrypted information by means of service

symbols; finding a mark that there is a copy of the electronic document, and a temporary individual number of the present document, recording the electronic document to the PROM and marking it with the assigned temporary individual number;

receiving the electronic-document-transmission-acknowledgement password to a personal cryptoprotective complex of a user who has received the electronic document copy, finding said electronic document copy marked with the number corresponding to the number received with the password in the PROM, and if the numbers coincide, removing the mark that there is a copy from the electronic document copy, and then recording the electronic document to the section of the PROM of the personal cryptoprotective complex, intended for non-copied electronic documents and closed for users of the PROM, and deleting said temporary individual number;

after the transmission of said password, deleting it from the PROM in the personal cryptoprotective complex of the sender of the electronic-document-transmission-acknowledgement password, and if a part of the password is transmitted with a variable face value, decreasing a face value of a part of said password residuary in the PROM by the sum equal to the transmitted part.

62. (New) A method for transmission of information with protection against copying with use of a personal cryptoprotective complex, the method comprising:

in a ROM of each of personal cryptoprotective complexes, storing copies of a mother code being a set of random numbers (M1, M2, ..., MN), encryption, decryption and information processing programs, wherein record is carried out in a protected way only in said personal cryptoprotective complexes, said way excluding the possibility of recording to other media and modifying said programs;

storing an individual number of the personal cryptoprotective complex as well as other attributes used for execution of cryptoprotective operations in the ROM and setting date and time in a built-in clock;

generating a decryption password on the basis of a random number and recording it to a section of a PROM intended for non-copied decryption passwords and closed for users;

generating a dynamically transformable daughter code on the basis of the mother code and the decryption password;

inputting information, including a computer program, to the personal cryptoprotective complex, and making its encryption using said decryption password;

outputting the encrypted information to a user for record to a medium or for transmission to other user;

inputting a command to transmit the decryption password to other user in process of the protected communication session;

encrypting the decryption password on the basis of a single-use key generated using at least one random number, and outputting said password for transmission;

according to the fact that the decryption password has the status of a non-copied electronic document, upon termination of transmission of the present electronic document, disabling it for a predetermined time period T1 in the PROM;

receiving the electronic document and decrypting the electronic document, establishing the reliability of information by check for absence of distortions in said information,

searching for and selecting service information from decrypted information by means of service symbols, using the service symbols to find the service information containing an electronic document inability-for-copying command, recording the electronic document to the section of the PROM intended for non-copied electronic documents, and disabling said document for the predetermined time period T2;

generating an electronic-document-loading-acknowledgement password in the personal cryptoprotective complex of a receiving party and transmitting the electronic-document-loading-acknowledgement password in the encrypted form to the personal cryptoprotective complex of a sending party;

in case if the sender does not receive the electronic-document-loading-acknowledgement password from the recipient

during the time period T1, enabling the electronic document in the PROM of the personal cryptoprotective complex of the sender, while ignoring the subsequent reception of said password;

in case if the recipient does not send the electronic-document-loading-acknowledgement password to the sender during the time period T1, deleting the electronic document from the PROM of the personal cryptoprotective complex;

receiving the electronic-document-loading-acknowledgement password in the personal cryptoprotective complex of the sending party, generating an electronic-document-transmission-acknowledgement password, and requesting a user acknowledgement in response to the sending of the present password to the personal cryptoprotective complex of the receiving party;

in case if the user gives no acknowledge in response to the sending of the password during the predetermined time period T2, then, on the expiration of said time period, automatically enabling said electronic document in the PROM of the personal cryptoprotective complex of the sender, and automatically deleting said electronic document in the PROM of the personal cryptoprotective complex of the recipient;

in case if the user acknowledges the sending of the password during the time period T2, sending the present password in the encrypted form to the personal cryptoprotective complex of the recipient, wherein said electronic document is automatically deleted from PROM of the personal cryptoprotective complex of the sender, and said electronic document is automatically enabled in the PROM of the personal cryptoprotective complex of the recipient when he or she has received said electronic-document-transmission-acknowledgement password;

recording the decryption password to the section of the PROM intended for non-copied electronic documents and closed for users of the PROM;

inputting information, including a computer program, to the personal cryptoprotective complex and decryption said information on the basis of the dynamically transformable code generated using the decryption password read out of the PROM;

in case of decryption of a computer program, connecting the personal cryptoprotective complex to a computer, recording a decrypted fragment of the program to a RAM of the personal cryptoprotective complex, executing only a part of operations in a microprocessor of the personal cryptoprotective complex compatible to the computer, while executing another part in the microprocessor of the computer.

63. (New) The method according to claim 62, further comprising:

inputting a user's command to limit a validity period of the decryption password in time or quantity of events of use;

including appropriate service commands in the decryption password and selecting them by means of service symbols;

encrypting the received service commands in structure of the decryption password, and outputting them for the further record to a medium or transmission to other user while storing the decryption password in the PROM,

simultaneously disabling the access to the decryption password residuary in the PROM of the personal cryptoprotective complex of the user for a predetermined time interval;

inputting or accordingly receiving the encrypted decryption password with service commands included therein;

selecting service commands by means of service symbols, and executing operations with the present decryption password according to the received commands from the service information, exactly: deleting the decryption password from the memory of the personal cryptoprotective complex after the expiration of time pointed in the service information or after use of the decryption password as much times as indicated in the service information.

64. (New) The method according to claim 62, further comprising:

inputting a command to transmit the decryption password to other user in an encrypted electronic letter;

adding service information separated by means of service

symbols to the decryption password, with the indication of the individual number of the personal cryptoprotective complex of the recipient, and also of date and time after which expiration the recipient of the present decryption password can transmit said password to other users of personal cryptoprotective complexes;

simultaneously, generating an electronic letter in the personal cryptoprotective complex of the sender of the decryption password, said letter including the decryption password with the service information added thereto, with additional indication of the date and time in the form of service information as well, and the personal cryptoprotective complex of the electronic letter recipient will be able to decrypt said message only before the expiration of said date and time, wherein the date and time of decrypting the electronic letter should be indicated earlier than or identical to the date and time indicated in the service information of the decryption password;

encrypting the generated electronic letter with the dynamically transferable code based on the single-use key generated from a random number and the individual number of the personal cryptoprotective complex of the recipient of the present electronic letter, and adding said random number to the encrypted electronic letter;

outputting the encrypted electronic letter and the random number for transmission to the addressee together with information decrypted by means of the decryption password;

recording the encrypted electronic letter containing the decryption password together with the random number to a medium or transmitting said letter through a communication link, and upon termination of transmission, deleting the encryption password from the PROM of the personal cryptoprotective complex of the sender;

receiving the encrypted electronic letter, the random number and the encrypted information;

inputting the random number to the RAM of the personal cryptoprotective complex, and reading the individual number of the personal cryptoprotective complex out of the ROM and

recording it to the RAM as well;

generating a single-use key on the basis of the inputted random number and the read-out individual number;

generating the dynamically transformable code on the basis of the single-use key and inputting the encrypted electronic letter to the personal cryptoprotective complex;

decrypting the electronic letter using the dynamically transformable code and recording the decrypted text of the electronic letter to the RAM;

defining service information by means of service symbols, finding the service information with indication of the final date and time of decrypting the electronic letter and collating them with the date and time in the built-in clock, and in case if the final date and time are later than the current date and time, deleting the present electronic letter from the RAM;

finding the decryption password, which includes the date and time after which expiration the decryption password may be transmitted to other users, and recording said decryption password to the section of the PROM of the personal cryptoprotective complex, intended for non-copied decryption passwords and closed for users of the PROM;

inputting information, including a computer program, to the personal cryptoprotective complex and decrypting said information on the basis of the dynamically transformable code generated using the decryption password read out of the PROM;

wherein, after the expiration of date and time pointed in the service information included in the decryption password, deleting the present service information from the PROM, with simultaneous removal of the restriction on the further transmission of the decryption password to other users.

65. (New) The method according to claim 62, further comprising:

adding a temporary individual number generated by a random-number generator to the electronic document, and an arbitrary inputted value of the time period T2, said number and value being

encrypted together with the electronic document;

inputting a command to transmit the electronic document to other user during the protected communication session or in the encrypted electronic letter;

when the transmission of the present electronic document terminates, disabling said document for a predetermined time period T1 in the PROM of the sender and marking said document with an assigned temporary individual number;

in case of failures in transmission of the electronic document, the sender repeatedly sends the present electronic document with the same accompanying data;

receiving the electronic document and decrypting the electronic document, establishing the reliability of information by check for absence of distortions in the information;

searching for and selecting service information from the decrypted information by means of service symbols, using service symbols to find service information containing an electronic document inability-for-copying command and the temporary individual number of the present document; collating said number for presence of a disabled electronic document having the same number in the PROM, and in case if coincidence is absent, recording the electronic document to the section of the PROM intended for non-copied electronic documents, marking it with the assigned temporary individual number and disabling the electronic document for the predetermined time period T1;

in the personal cryptoprotective complex of the receiving party, generating an electronic-document-loading-acknowledgement password on the basis of a random number, automatically adding said temporary individual number of the present electronic document to said password, recording a password to the PROM, and transmitting the electronic-document-loading-acknowledgement password in the encrypted form to the personal cryptoprotective complex of the sending party during the protected communication session or in the encrypted electronic letter;

receiving the electronic-document-loading-acknowledgement password in the personal cryptoprotective complex of the sending

party, finding the disabled electronic document in the PROM, said document being marked by number corresponding to a number received with the password, and in case of presence of the disabled electronic document and coincidence of numbers there is the step of generating an electronic-document-transmission-acknowledgement password with use of electronic-document-loading-acknowledgement password, said temporary individual number of the electronic document being automatically included therein;

requesting a user acknowledgement for sending said password to the personal cryptoprotective complex of the receiving party;

in case if the user does not give acknowledgement for sending the password during an arbitrary time period T2 which value was inputted beforehand by the sender in establishment of an electronic document sending mode, then after the expiration of a predetermined period of time there are the steps of: automatically enabling said electronic document in the PROM of the personal cryptoprotective complex of the sender; and automatically deleting said electronic document in the PROM of the personal cryptoprotective complex of the recipient;

in case if the user gives acknowledgement for sending the password during the time period T2, then sending said password in the encrypted form to the personal cryptoprotective complex of the recipient, wherein said electronic document is automatically deleted from the PROM of the personal cryptoprotective complex of the sender, and when the recipient has received the electronic-document-transmission-acknowledgement password, there is the step of finding the disabled electronic document and the recorded copy of the electronic-document-loading-acknowledgement password in the PROM of the personal cryptoprotective complex of the recipient, said document and said copy being denoted by number corresponding the number received with the password, and only in case of presence of the disabled electronic document, coincidence of numbers and presence of a direct association between passwords, said electronic document is automatically enabled;

recording the electronic document to the section of the PROM of the personal cryptoprotective complex, intended for non-copied

electronic documents and closed for users of the PROM, and deleting said temporary individual number;

in case of failures in transmission of the electronic document or acknowledgement passwords, users carry out the backup of transmission.

66. (New) The method according to claim 65, further comprising:

adding an individual number N1 of the personal cryptoprotective complex where from the electronic-document-transmission-acknowledgement password will be sent, a temporary individual number N2 generated by the random-number generator, and an infinite value T2 of the time period to be inputted by the user, said number and value being encrypted together with the electronic document, to the transmittable electronic document;

inputting a command to transmit the electronic document to other user in process of the protected communication session;

when the transmission of the present electronic document terminates, enabling said document for a predetermined time period T1 in the PROM of the sender and marking said document with said assigned number N2;

receiving the electronic document and decrypting the electronic document, establishing the reliability of information by check for absence of distortion in information;

searching for and selecting service information from the decrypted information by means of service symbols, using said service symbols to find service information containing an electronic document inability-for-copying command and numbers of said document, recording the electronic document to the section of the PROM intended for non-copied electronic documents, marking said document with its assigned number N2 and disabling the electronic document for the predetermined time period T1;

in the personal cryptoprotective complex of the receiving party, generating the electronic-document-loading-acknowledgement, automatically adding said number N2 of the present electronic document to said password and transmitting the

result in the encrypted form to the personal cryptoprotective complex of the sending party during the same or other protected communication session;

receiving the electronic-document-loading-acknowledgement of the electronic document in the personal cryptoprotective complex of the sending party, finding the disabled electronic document in the PROM, said document being marked by number N2 corresponding to the number received with the password, and in case of presence of the disabled electronic document and coincidence of numbers, deleting the present electronic document from the PROM, because the time period T2 is equal to an infinite value;

in the personal cryptoprotective complex whose individual number corresponds to the number N1 assigned to the electronic document, inputting a numerical value corresponding to the number N2 of the electronic document, generating the electronic-document-transmission-acknowledgement password while automatically including therein own individual number corresponding to N1 and the inputted number N2;

sending the present password in the encrypted to the personal cryptoprotective complex of the recipient of the electronic document;

when the personal cryptoprotective complex of the recipient has received the electronic-document-transmission-acknowledgement password in its PROM, finding the disabled electronic document marked by the number N2 corresponding to the number received with the password, collating the numbers N1 in the electronic document and in the password, and only if coincidence of numbers takes place, automatically enabling said electronic document;

recording the electronic document to the section of the PROM of the personal cryptoprotective complex, intended for non-copied electronic documents, and deleting the added numbers N1 and N2.

67. (New) The method according to claim 65, further comprising:

adding the temporary individual number generated by the random-number generator and an infinite value T2 of the time

period, said number and value being encrypted together with the electronic document, to the transmittable electronic document;

inputting a command to generate said electronic-document-transmission-acknowledgement password;

generating an electronic-document-acknowledgement password, assigning a number and a variable face value, if any, thereto, said number and variable face value corresponding to the temporary number and temporary face value of the electronic document;

transmitting the electronic-document-acknowledgement password in the encrypted form during a cryptoprotective communication session to a certain user or keeping said password in own personal cryptoprotective complex;

disabling the electronic document for an arbitrary time period T1 in the PROM of the personal cryptoprotective complex, making copies of the electronic document and transmitting them to other users in process of the cryptoprotective communication session or in an encrypted electronic letter;

after the expiration of the time period T1, deleting the electronic document from the PROM of the sender;

receiving copies of the electronic document, decrypting the electronic document, searching for and selecting service information from the decrypted information by means of service symbols; finding a mark that there is a copy of the electronic document, and a temporary individual number of the present document, recording the electronic document to the PROM and marking it with the assigned temporary individual number;

receiving the electronic-document-transmission-acknowledgement password to a personal cryptoprotective complex of a user who has received the electronic document copy, finding said electronic document copy marked with the number corresponding to the number received with the password in the PROM, and if the numbers coincide, removing the mark that there is a copy from the electronic document copy, and then recording the electronic document to the section of the PROM of the personal cryptoprotective complex, intended for non-copied

electronic documents and closed for users of the PROM, and deleting said temporary individual number;

after the transmission of said password, deleting it from the PROM in the personal cryptoprotective complex of the sender of the electronic-document-transmission-acknowledgement password, and if a part of the password is transmitted with a variable face value, decreasing a face value of a part of said password residuary in the PROM by the sum equal to the transmitted part.

68. (New) A method for simultaneously exchanging copy-protected electronic documents among users through a communication link with use of a cryptoprotective complex, comprising:

in a ROM of each of personal cryptoprotective complexes, storing copies of a mother code being a set of random numbers (M1, M2, ..., MN), encryption, decryption and information processing programs, wherein record is carried out in a protected way only in said personal cryptoprotective complexes, said way excluding the possibility of recording to other media and modifying said programs;

storing an individual number I of the personal cryptoprotective complex in the ROM as well as personal data of a user including his or her electronic signature and other attributes used for execution of cryptoprotective operations and generation of electronic documents, and setting date and time in a built-in clock;

synchronously generating a single-use encryption key on the basis of random numbers produced in the personal cryptoprotective complexes of users;

synchronously generating dynamically transformable daughter codes on the basis of the mother code and the single-use encryption key in the personal cryptoprotective complexes of users;

inputting initial information to each of the personal cryptoprotective complexes of users; in accordance with an established mode of processing user's information and earlier

received information, generating service information by means of the information processing program and combining the service information with the processed user's information to obtain an electronic document, wherein attributes of the electronic document in the form of service information are separated from the processed user's information by means of predetermined service symbols, and in accordance with a user's command to generate a copy-protected electronic document, including a certain command in the service information as a part of the information processing program for the personal cryptoprotective complexes, wherein said command is in the form of a typical set of symbols earlier inputted to the ROM, and storing the obtained electronic document in a section of the PROM provided in the personal cryptoprotective complex and intended for non-copied electronic documents;

in at least one of the personal cryptoprotective complexes, inputting a command for simultaneous exchanging the electronic documents, and sending said command in the form of a signal encrypted by means of the produced single-use encryption key to other personal cryptoprotective complex;

in each of the personal cryptoprotective complexes, inputting a command to start transmission of the non-copied electronic document recorded in the PROM to other subscriber of the established communication session;

encrypting the electronic document with a dynamically transformable daughter code while reading an electronic document inability-for-copying command out of the service information; establishing protection against modification in the decrypted information and transmitting the encrypted information to other personal cryptoprotective complex;

in accordance with the command for simultaneous exchanging the electronic documents, and upon termination of transmission of the non-copied electronic document, disabling it for a predetermined time period T1 in the PROM of the sender;

receiving the electronic document and decrypting the electronic document, establishing the reliability of information

by check for absence of distortions in information;

searching for and selecting service information from the decrypted information by means of service symbols, using the service symbols to find service information containing the electronic document inability-for-copying command, recording the electronic document to the section of the PROM intended for non-copied electronic documents, disabling said electronic document for a predetermined time period T1 and outputting the obtained electronic document to the user for acquaintance;

in the personal cryptoprotective complex of the receiving party, generating an electronic-document-loading-acknowledgement password and transmitting said electronic-document-loading-acknowledgement password in the encrypted form to the personal cryptoprotective complex of the sending party;

if the sender does not receive the electronic-document-loading-acknowledgement password from the recipient during the time period T1, the electronic document is enabled in the PROM of the personal cryptoprotective complex of the sender;

if the recipient does not send the electronic-document-loading-acknowledgement password to the sender during the time period T1, deleting the electronic document from the PROM of the personal cryptoprotective complex of the recipient;

receiving the electronic-document-loading-acknowledgement in the personal cryptoprotective complex of sending party, generating an electronic-document-transmission-acknowledgement password and requesting a user acknowledgement to send the present password to the personal cryptoprotective complex of the receiving party;

in case if the user does not acknowledge the sending of the password during a predetermined time period T2, then, after the expiration of said time period, automatically enabling said electronic document in the PROM of the personal cryptoprotective complex of the sender, and automatically deleting said electronic document in the PROM of the personal cryptoprotective complex of the recipient;

in case if the user gives the acknowledgement for sending

the password during the time period T2, then, sending a predetermined signal in the encrypted form containing information of said acknowledgement to other user, and receiving the similar signal from said user;

after the exchange of acknowledgement signals, making synchronization according the last signal, and from the moment of sending a last bit of said signal from one of personal cryptoprotective complexes and to the moment of according reception thereof in other personal cryptoprotective complex, starting a procedure of a simultaneous exchange of the electronic-document-transmission-acknowledgement passwords in the encrypted form, wherein the reception of a password-containing signal from the opposite party is monitored in each of the personal cryptoprotective complexes, and in case of absence or interruption of said signal, the transmission of own password is stopped;

after the sending of the transmission-acknowledgement password, automatically deleting said electronic document from the PROM of the personal cryptoprotective complex of the sender, and when the recipient has received the electronic-document-transmission-acknowledgement password, automatically enabling said electronic document in the PROM of the personal cryptoprotective complex of the recipient.

69. (New) The method according to claim 68, further comprising:

automatically introducing a time value T to the last acknowledgement signal, said value being different from a current time-reading by a time period t which value is generated by the random-number generator;

sending the present signal to other user, and after the expiration of the signal sending time and before the time T comes, transmitting a random signal generated by the random-number generator;

when the time T comes, automatically stopping transmission of the random signal and starting simultaneous transmission of

electronic-document-transmission-acknowledgement passwords in the encrypted form, said random signal and the cryptogram of passwords having identical characteristics.

70. (New) The method according to claim 68, wherein

users make an exchange of a copy of the electronic document preliminary signed by everyone with his or her own electronic digital signature, and after reception, disabling in the PROM and acquaintance with the received electronic documents, at least one of users inputs a command of simultaneous signing the present electronic document;

a signal in the encrypted form is sent to other user, said signal containing information on simultaneous signing the electronic document and being outputted to the user;

after the exchange of the electronic-document-transmission-acknowledgement passwords, there is the step of automatically signing the electronic documents in each of the personal cryptoprotective complexes with the electronic digital signature of the user.

71. (New) The method according to claim 68, further comprising:

inputting, in one of the personal cryptoprotective complexes, a command to send an electronic letter at notice and inputting information, adding a number generated by the random-number generator to the present information, separating said number by means of earlier inputted service symbols and encrypting the information by said number with application of a decryption password;

in accordance with said command, recording the decryption password to the PROM of the personal cryptoprotective complex and marking said passwords with said number;

generating the electronic letter at notice from the inputted encrypted information and the service information added thereto, separated with earlier inputted service symbols, containing the number that corresponds to a number of information and the

decryption password, and having a command included therein and indicating that the present information is an electronic letter at notice, outputting a copy of the encrypted electronic letter at notice for record to a medium;

establishing a cryptoprotective communication session with a certain user using the personal cryptoprotective complexes, and transmitting the electronic letter at notice;

receiving information; decrypting the service information, finding the number to be recorded to the PROM, and a command that the received encrypted information is an electronic letter at notice, and outputting the present command to the user;

in accordance with said command and a command inputted by the recipient – to send a notice on reception of said message to the sender, generating the electronic document in the form of a preliminary inputted typical notice sheet, inputting the number to said sheet, said number corresponding to a number of the received information; and signing the present electronic document with an electronic signature of the user, said signature containing the current date and time;

sending a predetermined signal in the encrypted form to other user, said signal containing information that acknowledges presence of the notice;

after the sending and respective reception of said signal, simultaneous changing the electronic notice sheet for an electronic letter decryption password;

receiving said decryption password to the personal cryptoprotective complex of the recipient, using said password to decrypt information received in the electronic letter at notice and outputting said information to the user;

receiving the electronic document being the notice-of-reception sheet of the electronic letter at notice to the personal cryptoprotective complex of the sender, decrypting said electronic document and inputting it to the user and recording a cryptogram of the notice sheet to the medium.

72.   (New)   The   method   according   to   claim   68,   further

comprising:

inputting, in the personal cryptoprotective complex of the sender, a command to send an electronic letter at notice and inputting information, adding a number N generated by the random-number generator to the present information, separating said number by means of earlier inputted service symbols, inputting an individual number I of the personal cyrptoprotective complex of the addressee, producing a random number Z;

based on the inputted number I and the random number Z, encrypting the information, including the added random number N;

in accordance with said command, recording the random number Z to the PROM of the personal cryptoprotective complex and marking it with said random number N;

generating the electronic letter at notice from the inputted encrypted information and service information added thereto, separated with earlier inputted service symbols, containing the number that corresponds to the number N of information, and having a command included therein and indicating that the present information is an electronic letter at notice; outputting a copy of the encrypted electronic letter at notice for record to the medium;

transmitting the electronic letter at notice to a node computer, establishing a cryptoprotective communication session with a node cryptoprotective complex connected to the node computer, transmitting the random number Z to be stored in the node cryptoprotective complex;

receiving the electronic letter at notice from the node computer to the personal cryptoprotective complex of the addressee, decrypting the service information, finding the number N to be recorded to the PROM, and a command that the received encrypted information is an electronic letter at notice; and outputting the present command to the user;

in accordance with said command and a command inputted by the recipient - to send a notice on reception of said message to the sender, generating the electronic document in the form of a preliminary inputted typical notice sheet, inputting the number N

to said sheet, said number corresponding to a number of the received information; and signing the present electronic document with the electronic signature of the user, said signature containing the current date and time;

sending a predetermined signal in the encrypted form to the node cryptoprotective complex via the node computer, said signal containing information that acknowledges presence of the notice;

after the sending and respective reception of said signal, simultaneous changing the electronic notice sheet for the random number Z;

receiving the random number Z to the personal cryptoprotective complex of the recipient, outputting the individual number I of the personal cryptoprotective complex and generating a single-use decryption key of the basis of said numbers;

decrypting information received in the electronic letter at notice and outputting said information to the user;

receiving the electronic document being the notice-of-reception sheet of the electronic letter at notice to the personal cryptoprotective complex of the sender from the node cryptoprotective complex via the node computer, decrypting said electronic document and inputting it to the user and recording a cryptogram of the notice sheet to the medium.

73. (New) A cassette for a personal cryptoprotective complex, intended for protection and storage of confidential and cryptographic information, comprising:

a microchip including a microprocessor capable of suppressing and masking self-microradiations and creating false microradiations,

a nonvolatile memory for storing encryption, decryption and information processing programs and an individual number of a cryptoprotective device,

a volatile memory being for storing a mother code and comprising a built-in accumulator,

a protective sheath of the microchip, connected to the

accumulator and a protective sheath integrity monitor unit providing erase of information from the volatile memory at an authorized access from the outside, said protective sheath consisting of three layers wherein the inner and outer layers of the protective sheath are formed with light-reflecting surfaces faced each other, and a third, transparent layer enclosed there between, wherein the light-emitting microdiodes and microphotocells face to the outer light-reflecting layer, said protective sheath integrity monitor unit being intended to set a periodicity and a radiation doze of the light-emitting microdiodes, to measure power absorbed by the microphotocells, to compare the measured values to reference values, and at their non-coincidence to de-energize the volatile memory for destroying the mother code stored therein.

74. (New) A cassette according to claim 73, wherein the microprocessor comprises additional parallel paths to supply signals compensating the microradiations of own signals of the microprocessor, and a generator for generating false microradiations in a frequency band of self-microradiations of the microprocessor.